01 범죄의 역사로 보는 보안

01. 범죄의 역사로 보는 보안

학습 목표

사이버 범죄의 역사적 발전 과정을 통해 보안의 진화를 이해하고, 각 시대별 주요 보안 위협과 대응 방식의 변화를 학습합니다. AI 시대가 가져온 새로운 보안 패러다임을 이해합니다.

Preview

범죄의역사로보는보안

보안을 바라보는 관점

Static Perfectness will always be broken

완벽하다고 생각하는 순간 오류

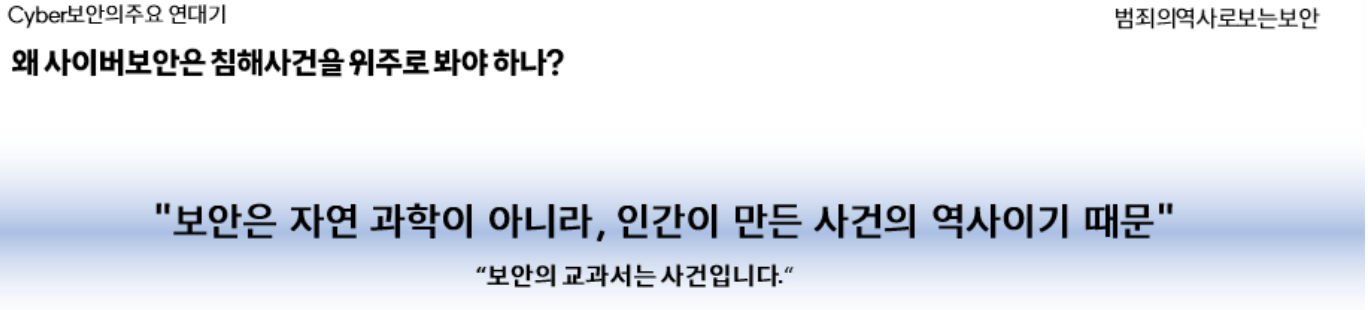
온전한 차단은 죽음

과거의 데이터로 경계에 발을 딛고 미래의 확률을 가늠한다

4

1.1 개요

정보보안의 역사는 기술 발전과 함께 진화해왔습니다. 1960년대 메인프레임 시대부터 현재의 AI 시대까지, 각 시기마다 새로운 위협과 방어 기술이 등장했습니다. 이 장에서는 시대별 주요 사이버 범죄 사례와 그 의미를 살펴봅니다.



Cyber보안의주요 연대기

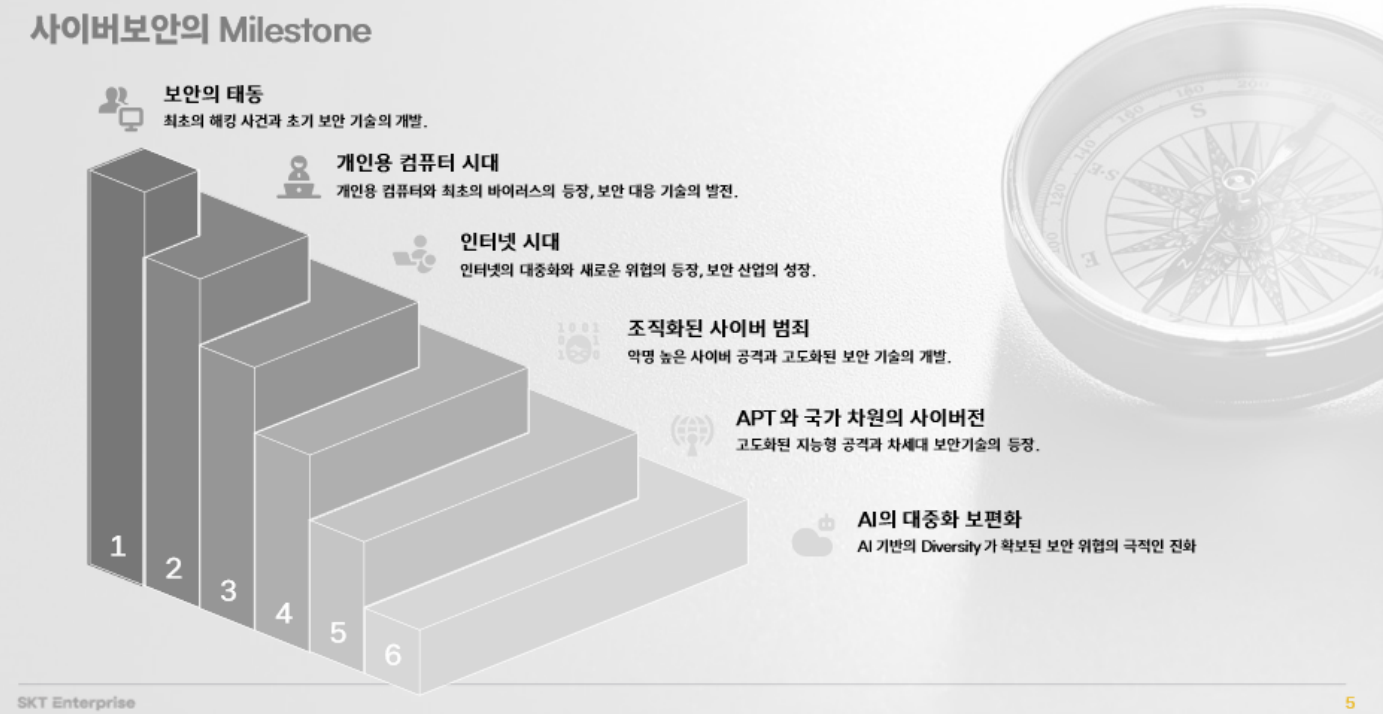
범죄의역사로보는보안

왜 사이버보안은 침해사건을 위주로 봐야 하나?

"보안은 자연 과학이 아니라, 인간이 만든 사건의 역사이기 때문"

"보안의 교과서는 사건입니다."

사이버보안의 Milestone



1.2□□ □□ □□ □□

1.2.1□□ (1960~1970□)

1960년대-1970년대: 보안의 태동기

전화 망 통신 해킹

최초의 해킹 사건들

- **1960년대 MIT**: 전화 프리킹(Phone Phreaking)이 시작되며 최초의 해커 문화가 형성
- **1971년: 존 드레이퍼(John Draper)가 시리얼 박스 휘슬을 이용한 전화 해킹으로 "캡틴 크런치"라는 별명 획득**
- **1973년**: 최초의 컴퓨터 침입 사건 - 로버트 모리스가 벨 연구소 시스템에 무단 접근

초기 보안 기술

- **1970년**: 암호화 연구가 본격화되며 DES(Data Encryption Standard) 개발 시작
- **1976년**: 디피-헬먼(Diffie-Hellman) 공개키 암호화 알고리즘 발표
- **1977년**: RSA 암호화 알고리즘 개발 - 현재까지 사용되는 공개키 암호화의 기초

Phone Phreaking의 시대

전화 시스템의 취약점을 이용한 초기 해킹 문화가 형성되었습니다. 순수한 기술적 호기심과 시스템 탐구가 주된 동기였습니다.

1971년

Captain Crunch (John Draper)

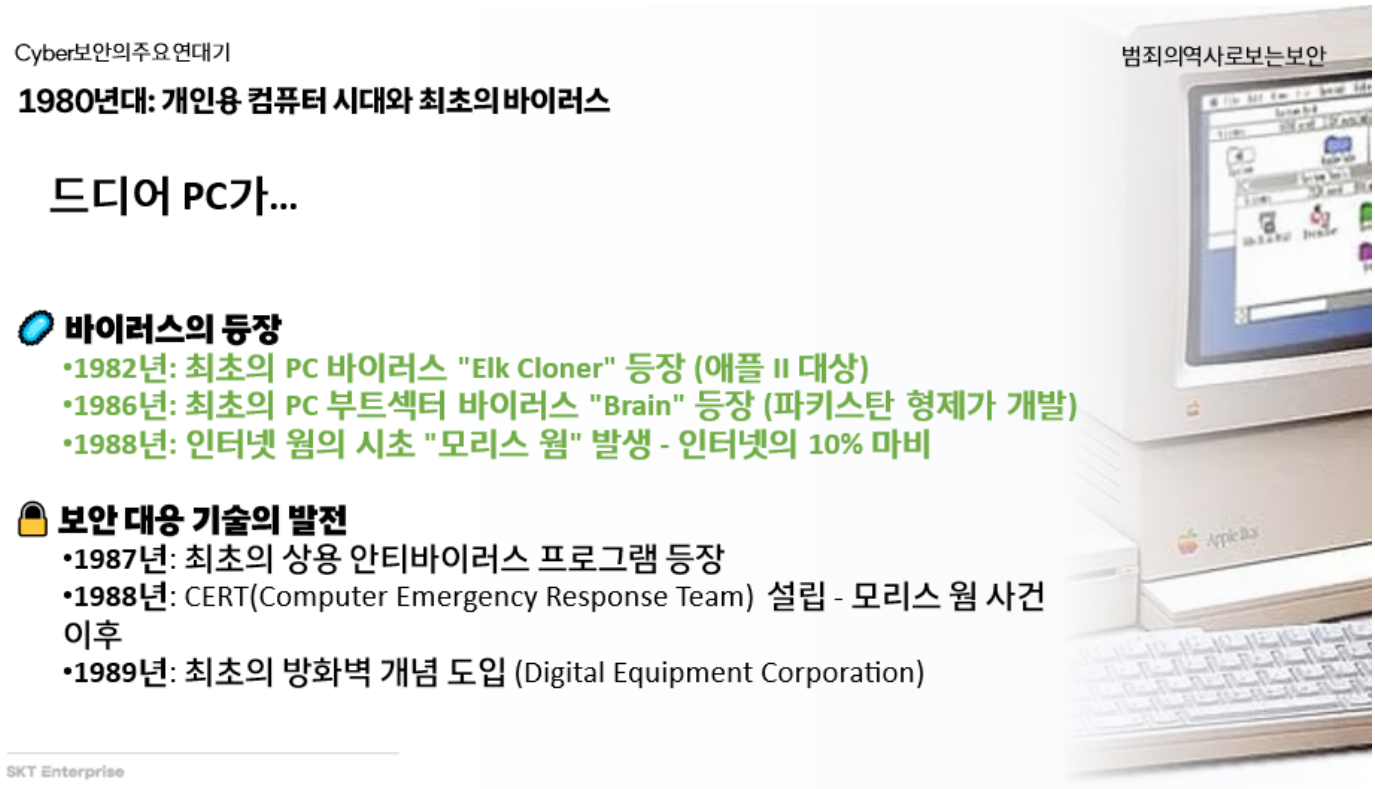
시리얼 상자에서 나온 장난감 호루라기가 2600Hz 톤을 생성한다는 것을 발견하고, 이를 이용해 AT&T 전화 시스템을 무료로 사용할 수 있게 되었습니다. 이는 Phone Phreaking의 시작이었으며, 해커 문화의 기원이 되었습니다.

1975년

Steve Wozniak & Steve Jobs의 Blue Box

애플의 창업자들도 젊은 시절 Blue Box라는 Phone Phreaking 장치를 제작하고 판매했습니다. Wozniak은 기술적 도전을, Jobs는 사업 기회를 보았습니다.

1.2.2 개인용 컴퓨터 시대 (1980년대)



Cyber보안의주요연대기

범죄의역사로보는보안

1980년대: 개인용 컴퓨터 시대와 최초의바이러스

드디어 PC가...

바이러스의 등장

- 1982년: 최초의 PC 바이러스 "Elk Cloner" 등장 (애플 II 대상)
- 1986년: 최초의 PC 부트섹터 바이러스 "Brain" 등장 (파키스탄 형제가 개발)
- 1988년: 인터넷 웜의 시초 "모리스 웜" 발생 - 인터넷의 10% 마비

보안 대응 기술의 발전

- 1987년: 최초의 상용 안티바이러스 프로그램 등장
- 1988년: CERT(Computer Emergency Response Team) 설립 - 모리스 웜 사건 이후
- 1989년: 최초의 방화벽 개념 도입 (Digital Equipment Corporation)

SKT Enterprise

1980년대는 개인용 컴퓨터의 보급과 함께 최초의 컴퓨터 바이러스가 등장한 시기입니다. 이 시기의 악성코드는 주로 실험적 성격이 강했습니다.

용어집 : 1980년대 주요 바이러스

① Elk Cloner (1982년)

- 15세 고등학생 Richard Skrenta가 Apple II용 플로피 디스크로 만든 세계 최초의 PC 바이러스
- 처음에는 장난 목적이었으나, 사용자 시스템에 의도치 않게 퍼져나감
- "컴퓨터도 생물학적 바이러스처럼 감염될 수 있다"는 사실을 대중에게 각인
- 50번째 부팅 시 화면에 시를 표시하는 무해한 동작

② Brain 바이러스 (1986년)

- 파키스탄의 두 형제 (Basit와 Amjad Alvi)가 개발한 최초의 IBM PC 부트 섹터 바이러스
- 불법 복제 소프트웨어 사용자를 추적하려는 목적으로 제작
- 감염된 디스크를 통해 퍼져나가며, 제작자의 이름과 연락처까지 코드에 포함
- "부트 섹터 감염"이라는 새로운 공격 방식을 개척

③ Morris Worm (1988년)

- Cornell 대학원생 Robert Tappan Morris가 만든 최초의 인터넷 웜
- 인터넷 규모를 측정하려던 실험이 통제를 벗어나 약 6,000대 (당시 인터넷의 10%) 감염
- 최초로 Computer Fraud and Abuse Act에 의해 기소된 사례
- 사이버 보안의 중요성을 각인시킨 분수령적 사건

1.2.3 인터넷 확산기 (1990년대)

Cyber보안의주요연대기

범죄의역사로보는보안

1990년대: 인터넷 대중화와 해킹의 진화

온라인을 통한 바이러스 확산

인터넷 시대의 새로운 위협

- **1994년**: 최초의 대규모 신용카드 정보 유출 사건
- **1995년: 케빈 미트닉 체포 - 당시 FBI의 최고 수배자**
- **1996년: 최초의 웹사이트 변조 사건들이 급증**

=> CIA 홈피 Central Stupidity Agency

- **1999년**: 멜리사 바이러스 - 이메일을 통한 대규모 확산

보안 산업의 성장

- **1991년**: PGP(Pretty Good Privacy) 공개 - 개인 암호화 도구의 대중화
- **1995년**: SSL(Secure Sockets Layer) 개발 - 웹 보안의 기초
- **1998년**: 침입탐지시스템(IDS) 상용화 시작
- **1999년**: PKI(Public Key Infrastructure) 표준화

상업적 목적의 악성코드 등장

1990년대 후반부터 악성코드가 단순한 장난이나 실험을 넘어 실질적인 피해를 입히는 도구로 변화했습니다.

연도	사건	특징	영향

1999	Melissa 바이러스	이메일을 통한 대량 확산	$80백만 피해, 이메일 보안 강화
2000	ILOVEYOU 웜	사회공학 기법 활용	전 세계 $100억 피해 추정
2001	Code Red	웹 서버 대상 공격	백악관 웹사이트 공격 시도
2003	SQL Slammer	10분 만에 전 세계 확산	한국 인터넷 대란 발생

1.2.4 조직 범죄화 (2000년대)

Cyber보안의주요연대기

범죄의역사로보는보안

2000년대: 사이버 범죄의 조직화

조직화 고도화 되는 사이버 범죄

💀 **악명 높은 사이버 공격들**

- •**2000년**: I LOVE YOU 바이러스 - 전 세계 수십억 달러 피해
- •**2001년**: 코드 레드 웜 - 백악관 웹사이트 공격 시도
- •**2003년: SQL 슬래머 웜 - 10분 만에 전 세계 확산**
- •**2004년**: 마이둠 웜 - 당시 가장 빠른 확산 속도 기록
- •**2008년: 컨피커 웜 - 1,500만 대 이상 감염**

🔐 **보안 기술의 고도화**

- •**2000년**: 침입방지시스템(IPS) 등장
- •**2003년**: 통합보안관리(UTM) 솔루션 개발
- •**2005년**: 웹 애플리케이션 방화벽(WAF) 상용화
- •**2007년**: 데이터 손실 방지(DLP) 기술 도입

SKT Enterprise

13

2000년대는 사이버 범죄가 조직화되고 산업화된 시기입니다. 금전적 이익을 목적으로 한 전문 범죄 조직이 등장했습니다.

봇넷과 지하경제의 형성

수백만 대의 좀비 PC를 관리하는 봇넷이 등장하고, 다크웹을 통한 사이버 범죄 도구와 정보 거래가 활성화되었습니다.

주요 변화

1. 금융 범죄의 증가
    - 온라인 뱅킹 해킹
    - 신용카드 정보 대량 탈취
    - 피싱 사이트를 통한 개인정보 수집
2. 봇넷의 등장
    - Storm 봇넷 (2007): 100만 대 이상 감염
    - Conficker (2008): 1,500만 대 감염 추정

    - DDoS 공격의 상품화
3. 랜섬웨어의 시작
    - GPCode (2005): 최초의 현대적 랜섬웨어
    - 암호화 기술을 이용한 데이터 인질
    - 익명 결제 시스템 (비트코인) 등장 전까지는 제한적

1.2.5 국가 차원의 위협 (2010년대)

Cyber보안의주요연대기

범죄의역사로보는보안

2010년대: APT와 State actor국가 차원의 사이버전

🎯 **고도화된 지능형 공격**

- **2010년: 스턱스넷(Stuxnet) - 최초의 사이버 무기, 이란 핵시설 공격**
- **2011년**: 익명(Anonymous) 그룹의 활동 활발화
- **2013년: 스노든 폭로 - 국가 차원의 사이버 감시 실태 공개**
- **2014년**: 소니 픽처스 해킹 - 북한 관련 추정
- **2016년**: 미국 대선 관련 사이버 공격 의혹
- **2017년**: 워너크라이 랜섬웨어 - 전 세계 30만 대 감염

🛡 **차세대 보안 기술**

- **2010년**: 샌드박스 기술 상용화
- **2012년**: SIEM(Security Information and Event Management) 고도화
- **2014년**: 제로 트러스트(Zero Trust) 보안 모델 제시
- **2016년**: AI 기반 보안 솔루션 등장
- **2018년**: SOAR(Security Orchestration, Automation and Response) 도입

SKT Enterprise 15

APT (Advanced Persistent Threat)의 등장

국가 차원의 지원을 받는 해킹 그룹들이 장기간에 걸쳐 은밀하게 진행하는 지능형 지속 공격이 본격화되었습니다.

2010년

Stuxnet

이란 핵시설의 원심분리기를 파괴한 최초의 사이버 무기. 물리적 파괴를 일으킨 첫 사례로 사이버전의 새로운 시대를 열었습니다.

2013년

Target 데이터 유출

4,000만 개 신용카드 정보와 7,000만 개인정보 유출. 공급망 공격의 위험성을 보여준 사례입니다.

2014년

Sony Pictures 해킹

북한 연루 의혹. 기업 전체 시스템 파괴와 내부 정보 유출. 사이버 공격이 물리적 전쟁 행위와 동등한 수준으로 다뤄지기 시작했습니다.

2017년

WannaCry 랜섬웨어

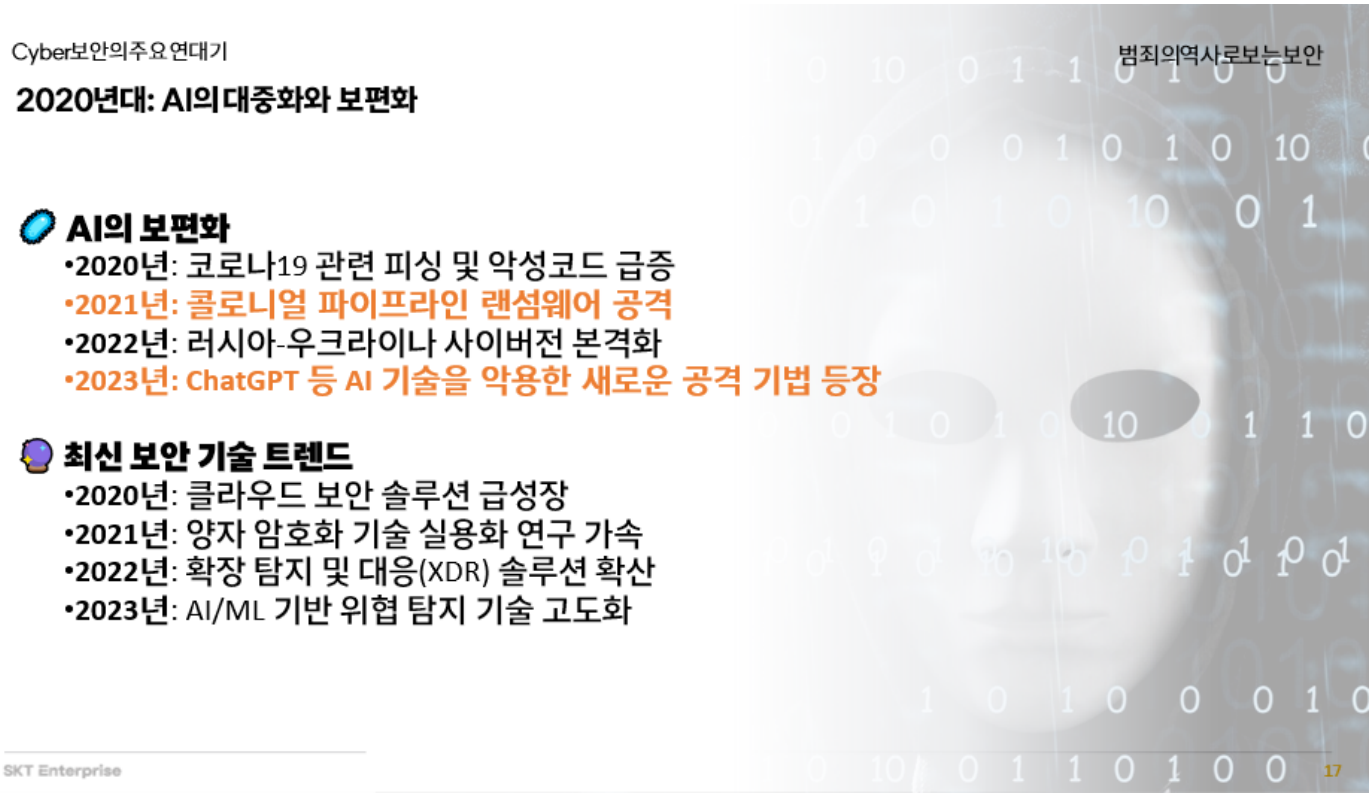
150개국 30만 대 이상 감염. NHS 병원 시스템 마비 등 실생활에 직접적 영향. EternalBlue 취약점 악용.

2020년

SolarWinds 공급망 공격

18,000개 이상 조직 영향. 러시아 APT 그룹 연루. 신뢰할 수 있는 소프트웨어 업데이트를 통한 침투.

1.3AI 시대의 보안 (2020년대 ~현재)



Cyber보안의주요연대기

범죄의역사로보는보안

2020년대: AI의 대중화와 보편화

AI의 보편화

- **2020년**: 코로나19 관련 피싱 및 악성코드 급증
- **2021년: 콜로니얼 파이프라인 랜섬웨어 공격**
- **2022년**: 러시아-우크라이나 사이버전 본격화
- **2023년: ChatGPT 등 AI 기술을 악용한 새로운 공격 기법 등장**

최신 보안 기술 트렌드

- **2020년**: 클라우드 보안 솔루션 급성장
- **2021년**: 양자 암호화 기술 실용화 연구 가속
- **2022년**: 확장 탐지 및 대응(XDR) 솔루션 확산
- **2023년**: AI/ML 기반 위협 탐지 기술 고도화

SKT Enterprise

17

1.3.1AI가 바꾸는 공격 패러다임

AI 기반 공격의 특징

- 자동화된 취약점 발견과 익스플로잇 생성
- 딥페이크를 활용한 정교한 사회공학 공격
- 머신러닝을 이용한 보안 시스템 우회
- 대규모 맞춤형 피싱 캠페인

AI 활용 공격 사례

1. DeepLocker (2018, IBM 연구)

AI를 이용해 특정 표적만을 식별하고 공격하는 악성코드. 얼굴 인식, 음성 인식, 위치 정보 등을 조합해 표적 확인.

2. GPT 기반 피싱 메일

대규모 언어 모델을 이용한 맞춤형 피싱 메일 자동 생성. 문법 오류가 없고 맥락에 맞는 내용으로 탐지 어려움.

3. Adversarial AI

AI 보안 시스템을 속이기 위한 적대적 예제 생성. 악성코드를 정상 파일로 인식하도록 유도.

1.3.2 AI 기반 방어 기술

AI가 강화하는 보안

- 행동 기반 이상 탐지 (UEBA)
- 제로데이 취약점 예측 및 방어
- 자동화된 위협 대응 (SOAR)
- 예측적 위협 인텔리전스

기술	설명	활용 분야
머신러닝 기반 탐지	패턴 학습을 통한 이상 행동 식별	악성코드 탐지, 침입 탐지
자연어 처리	피싱 메일, 악성 URL 분석	이메일 보안, 웹 보안
컴퓨터 비전	딥페이크 탐지, 생체 인증	신원 확인, 미디어 검증
강화학습	자동화된 보안 정책 최적화	방화벽 규칙, 접근 제어

1.4 보안 패러다임의 진화

1.4.1 전통적 보안 vs AI 시대 보안

패러다임 전환

구분	전통적 접근	**AI** 시대 접근
탐지 방식	시그니처 기반	행동 기반, 이상 탐지
대응 속도	수동적, 사후 대응	자동화, 실시간 대응
위협 예측	과거 데이터 의존	예측 모델링
보안 전략	경계 방어	Zero Trust

1.4.2 미래 전망

Quantum Computing과 보안

양자 컴퓨터의 등장은 현재의 암호화 체계를 무력화할 수 있습니다. Post-Quantum Cryptography 연구가 활발히 진행되고 있습니다.

향후 주요 도전 과제

1. **AI vs AI** 전쟁: 공격과 방어 모두 AI를 활용하는 자동화된 사이버전
2. 딥페이크와 신뢰의 위기: 진위 판별이 어려운 콘텐츠의 범람
3. **IoT** 보안: 수십억 개의 연결된 기기가 만드는 새로운 공격 표면
4. 개인정보와 프라이버시: AI의 데이터 의존성과 개인정보 보호의 균형
5. 규제와 거버넌스: AI 보안 기술의 윤리적 사용과 국제 협력

1.5 핵심 메시지

역사가 주는 교훈

사이버 보안의 역사는 공격과 방어의 끊임없는 진화 과정입니다. 각 시대의 기술 발전은 새로운 위협을 만들었지만, 동시에 새로운 방어 방법도 제시했습니다.

> "과거의 기억으로 현재의 경계에서 미래를 바라본다"
>
> - 보안의 역사를 이해하는 것은 미래의 위협에 대비하는 첫걸음입니다.

현재 우리의 위치

AI가 공격과 방어 양쪽에서 동시에 활용되는 시대에 살고 있습니다. 중요한 것은 기술 자체가 아니라, "인간과 AI가 어떻게 협력하여 불확실한 환경에서 최적의 의사결정을 내릴 것인가"입니다.

다음 장 예고:

*2*장 "급진적 변화의 시점에서"에서는 디지털 전환과 클라우드 시대가 가져온 보안 환경의 급격한 변화, 경계 기반 보안의 한계와 *Zero Trust* 모델의 등장, 그리고 현대 기업이 직면한 새로운 보안 과제들을 다룹니다.

Revision #6
Created 27 September 2025 03:30:53 by 최주용
Updated 27 September 2025 06:07:36 by 최주용